REMARKS

Reconsideration and re-examination of this rejection is respectfully requested in view of the above amendments and below remarks.

Objections to the claims

Claims 1 and 11 were objected to for various informalities. Applicants have amended the claims to overcome these rejections, and it is therefore requested that the objection be withdrawn. The Examiner is thanked for the careful review of the claims.

Double Patenting

Claims 1, 9, 11, 13 and 15 were rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims of co-pending application 10/661,657. Applicants acknowledge that a terminal disclaimer may be filed to overcome this rejection. However, because the claims of both applications are currently pending and subject to amendment, Applicants will delay determination as to whether a filing of the terminal disclaimer is a proper course of action until an allowable set of claims has been identified.

Rejections under 35 U.S.C. §112, second paragraph

Claims 13 and 15 were rejected under 35 U.S.C. §112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicant has cancelled claims 13-15 and thus submits that the rejection has been overcome and should be withdrawn.

Rejections under 35 U.S.C. §103

Claims 1, 6-9, 11 and 13-15 were rejected under 35 U.S.C. §103(a) as being unpatentable over Liu/Caronni et al. (U.S. Patent No. 6,970,941) in view of Hama et al. (U.S. Patent 7,072,346).

Liu:

Liu describes a method of enabling communications between a first private network and a second private network. As described in the Abstract of Liu: "...When communicating a packet from the first private network to the second private network, a computer receives a packet from a source node in the first private network. The computer then determines whether the packet is destined for the second private network. Thereafter, if the packet is destined for the second private network, the computer forwards the packet to a destination node in the second private network. When communicating a packet from the second private network to the first private network, a computer receives a packet from a source node in the second private network..."

Liu therefore describes a method and apparatus for communicating *between* private networks.

Caronni:

Caronni describes establishing a 'Supernet' which is a private network that uses components from a public-network infrastructure. At col. 4, lines 36-60 Caronni describes:

"... A Supernet allows an organization to utilize a public-network infrastructure for its enterprise network so that the organization no longer has to maintain a private network infrastructure; instead, the organization may have the infrastructure maintained for them by one or more service providers or other organizations that specialize in such connectivity matters. As such, the burden of maintaining an enterprise network is greatly reduced. ...

Supernets also provide heterogeneous addressing functionality. The Supernet uses a separate layer that isolates address names of nodes from addressing schemes and delivery

schemes. The Supernet contains a modification to the IP packet format that can be used to separate network behavior from addressing. As a result of the modification, any delivery scheme may be assigned to any address, or group of addresses...."

Caronni describes the address translation scheme in more detail at column 6, lines 6-25:

> "... the system provides address translation in a transparent manner. Since the Supernet is a private network constructed from the infrastructure of another network, the Supernet has its own internal addressing scheme, separate from the addressing scheme of the underlying public network. Thus, when a packet from a Supernet node is sent to another Supernet node, it travels through the public network. To do so, the Supernet performs address translation from the internal addressing scheme to the public addressing scheme and vice versa. By separating the addressing schemes, the Supernet creates a flexible delivery scheme that is easily changeable by network software or a system administrator. ***To reduce the complexity of Supernet nodes, system-level components of the Supernet perform this translation on behalf of the individual nodes so that it is transparent to the nodes.*** Another benefit of the Supernets' addressing is that it uses an IP-based internal addressing scheme so that preexisting programs require little modification to run within a Supernet..."

The Supernet of Caronni is thus merely a virtual network layered on top of the Internet IP network. For example, as described in the Abstract of Caronni 'The virtual network uses a separate layer to create a modification to the IP packet format that is used to separate network behavior from addressing..."

Figure 4 of Caronni illustrates an embodiment of the Supernet, which includes multiple nodes 316, 318, 320 and 322 which communicate with each other via shared channels. As described at column 5, lines 7-11 of Caronni "... When communicating among themselves, the nodes 316, 381, 320 and 322 serve as end points for the communications..."

At column 12, lines 10-20, Caronni recites:

"... When encrypting the packet, the virtual source node address 642, the virtual destination node address 644, and the data may be encrypted (addressing section 660), but the source and destination real addresses 614, 616 (delivery scheme section 670) are not, so that the real addresses can be used by the public network infrastructure to send packets to the destination..."

Thus Caronni stresses the importance of maintaining real addresses to enable delivery across the public network infrastructure.

Hama:

Hama describes, in the Abstract:

"... In network for forming a VPN on a shared network and communicating via the VPN, a core network of the VPN is formed by an MPLS network, access networks for accessing the core network are formed by VLANs, and edge routers are provided between the MPLS network and VLANs for interfacing the MPLS network and the VLANs. A transmit-side edge router converts a packet, which enters from a VLAN, to an MPLS packet and transmits this MPLS packet to the MPLS network, A receive-side edge router converts the MPLS packet, which has been received from the MPLS network, to a VLAN packet and directs the VLAN packet to a VLAN that belongs to the same VPN as that of a VLAN on the transmit side...."

Hama describes, at column 9 line 62 – column 10 line 12:

"...More specifically, the transmit-side edge router converts a VID contained in a VLAN packet to a VPN label, which is a VPN identifier, finds a forwarding label for forwarding the packet along a prescribed route on the basis of the destination of the VLAN packet, imposes these labels in place of the VIN to generate an MPLS packet, and sends the MPLS packet to the MPLS network 110. The latter routes the MPLS packet to the target receive-side edge router over a preset route while the forwarding label of the packet is replaced. Upon receiving the MPLS packet from the MPLS network, a receive-side edge router removes the forwarding label, converts the VPN label to the original VID, adds this VID to the packet in place of the label to generate a VLAN packet and sends the VLAN packet to the VLAN indicated by the VID. As a result of this operation, a packet can be transmitted from a transmit-side VLAN belonging to a certain VPN to a receive-side VLAN belong to the same VPN..."

Therefore in Hama describes a system which maps VIDs in a VLAN packet to an MPLS labels. Applicants note that to do so, the VLAN VID must be available to the transmit-side edge

router. In addition, Hama describes that packets received at the edge router have *already* been transformed and encapsulated with a VID label, and this VID label is used to generate a VPN label. Thus while Hama provides some conversion prior to the edge node, it does not preserve the destination address as stated in the claims, and as required by Caronni.

In contrast, the claims of the present invention, as amended, now clearly recite: "...encapsulating a private address of a packet from the first member with a group header including a public address associated with the first member and a group address to generate a tunneled packet; *transforming, at a client edge device, the tunneled packet by first applying a group security association ... to the tunneled packet to provide a secure tunneled packet* and then *adding a header field to the secure tunneled packet,* the added header field including a gateway address associated with the first member of the private network and *a destination address* of the second member of the private network to provide a client transformed packet; forwarding the client transformed packet to a provider edge device; and replacing, at the provider edge device, a destination field of the packet with a group identifier associated with the private network for routing the packet across the backbone..."

The present invention, by transforming the packet prior to transfer over the backbone, increases the security of the data transfer because *not even the group information* can be determined from the packet. Rather, the only information that is available is a gateway address and a destination address. The provider can derive, from the gateway address, that the packet is a type that has been transformed, and can use the destination address to further transfer the packet across the backbone. No such structure is shown or suggested by the combination of Caronni, Liu and Hama.

The Examiner states, at page 6 of the office action:

"… It would have been obvious … to combine … Hama within the system of Caronni because (a) Caronni teaches providing a virtual network mechanism that maintains secure communications… and (b) Hama teaches providing a cost-effective and scalable VPN on a shared network by using an edge router…"

Applicant's Argument

The requirements for establishing a *prima facie* case of obviousness as set out in the MPEP Section 2143.01 require that the references when combined: (1) teach all of the claimed limitations; (2) that there be a motivation/reason to combine the references; and (3) that there be a reasonable expectation of success in realizing the claimed invention. (The third requirement is only relevant to claims covering chemical inventions, and therefore is not discussed below.)

Before setting forth a discussion of the prior art applied in the Office Action, it is noted that the United States Supreme Court recently addressed the motivation/reason requirement that an Examiner must satisfy in order to determine that the subject matter of a claim is obvious based on the combination of two or more references. Specifically, in the ruling in *KSR International Co. v. Teleflex Inc. et al.*, 550 U.S. (2007), the United States Supreme Court stated: "Often, it will be necessary ... to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was **an apparent reason** to combine the known elements in the fashion claimed by the patent at issue. To facilitate review, **this analysis should be made explicit**. ... it can be **important to identify a reason** that would have prompted a person of ordinary skill in the

relevant field to combine the elements in the way the claimed new invention does." (emphasis added) .

It is further noted that the opinion of the United States Supreme Court is explicitly mandated in the USPTO memo to the Technology Center Directors from Margaret A. Focarino, Deputy Commissioner for Patent Operations, on May 3, 2007, which states:

"Therefore, in formulating a rejection under 35 U.S.C. § 103(a) based upon a combination of prior art elements, **it remains necessary to identify the reason why a person of ordinary skill in the art would have combined the prior art elements in the manner claimed.**" (emphasis added)

It would appear to be the Examiner's contention that one would be motivated to modify Caronni/Liu to 'translate' the packets prior to delivery over the backbone. However, such a conclusion ignores the statement of Caronni, which endorses the use of real addresses for transporting the packet over the backbone. Accordingly, applicants would traverse the Examiner's conclusion that there is motivation for combining the references.

However, even if the references *could* be combined, Applicant respectfully notes that the combination still would neither describe nor suggest the limitations of the claims, which appends the group header to the packet, then transforms the packet, such that when the packet traverses the backbone, the group identifier will be secured. No such structure is shown or suggested buy the combination of references provided by the Examiner.

Accordingly, for at least the reason that the combination of Caronni/Liu and Hama fail to disclose "encapsulating a private address of a packet from the first member with a group header including a public address associated with the first member and a group address to generate a

tunneled packet … *transforming, at a client edge device, the tunneled packet* by first applying a group security association associated with the private network to the tunneled packet to provide a secure tunneled packet and then adding a header field to the secure tunneled packet, the added header field including a gateway address associated with the first member of the private network and a destination address…"

Accordingly, for at least the reason that the combination of references fails to describe or suggest several limitations of claim 1 it is requested that the rejection be withdrawn. Dependent claims 6-8 serve to further limit claim 1 and are thus allowable with claim 1.

With regard to claim 9, neither Caronni/Liu , Hama or the combination thereof either describe or suggest the limitation of "*…determining, responsive to a gateway address of a packet, whether a packet received from a client edge device at a provider edge device of the backbone has been transformed to* secure packet data transferred across the backbone…" Accordingly, for at least this reason it is requested that the rejection be withdrawn.

Claim 11 includes limitations similar to those of claim 1, and is therefore patentably distinct over the combination of Caronni, Liu and Hama for at least the reasons that the combination neither describes nor suggests "…a tunneling mechanism for encapsulating packets that are to be transferred to the backbone in a public address including a gateway address and a group address to provide a tunneled packet; and transform logic operable to apply a security association to the tunneled ~~each~~ packet and to append a header to the tunneled packet, the header including a gateway address and a destination address to provide a transformed packet for transmission by the client edge device to the backbone…" Accordingly it is requested that the rejection of claim 11 be withdrawn.

Conclusion:

Applicants have made a diligent effort to place the claims in condition for allowance. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Applicants' Attorney at the number listed below so that such issues may be resolved as expeditiously as possible.

For these reasons, and in view of the above amendments, this application is now considered to be in condition for allowance and such action is earnestly solicited.

Respectfully Submitted,

September 27, 2007
Date

/Lindsay G. McGuinness/
Lindsay G. McGuinness, Reg. No. 38,549
Attorney/Agent for Applicant(s)
McGuinness & Manaras LLP
125 Nagog Park
Acton, MA 01720
(978) 264-6664

Docket No. 120-161
Dd: 9/23/2007